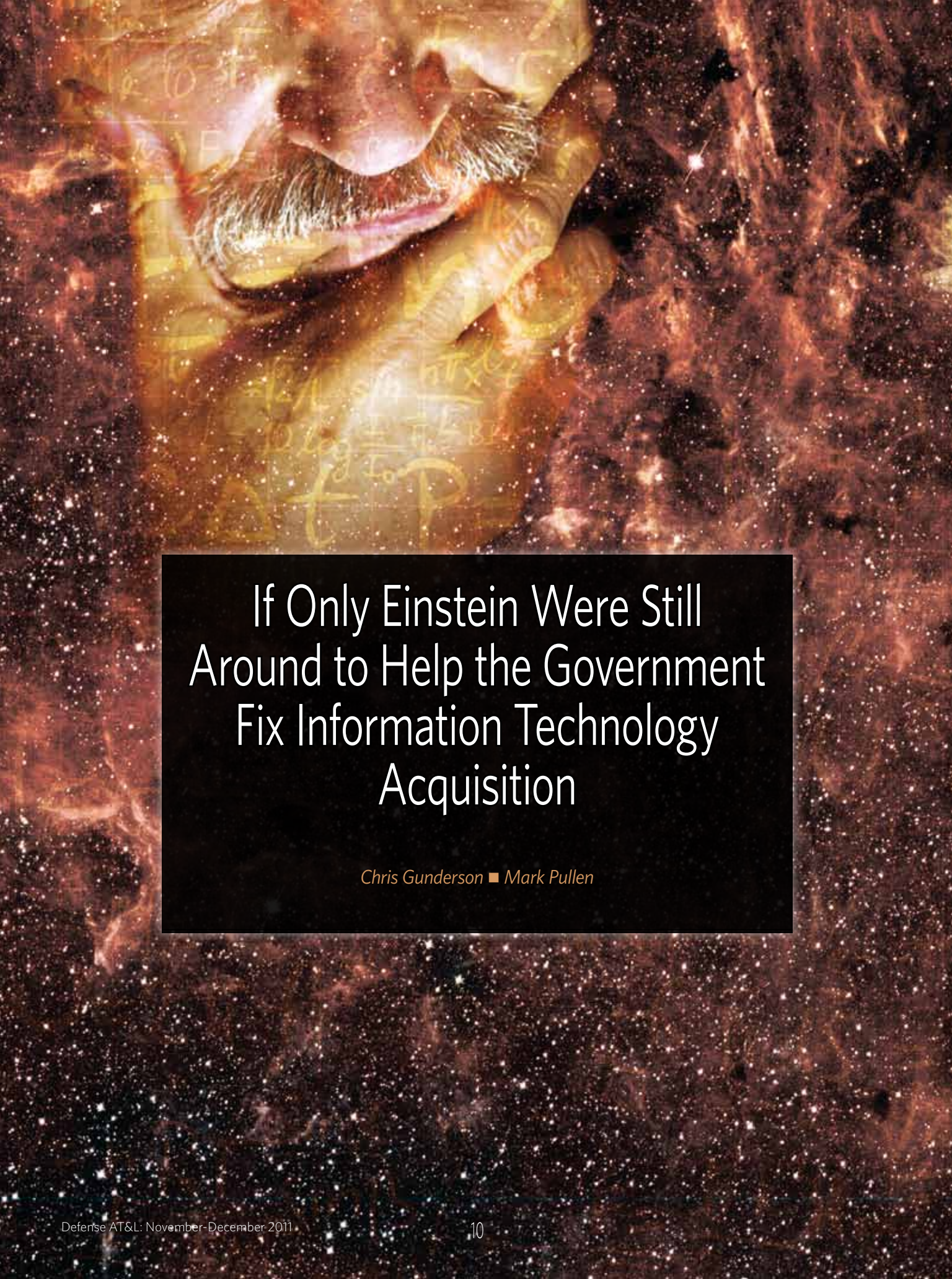

If Only Einstein Were Still Around to Help the Government Fix Information Technology Acquisition

Chris Gunderson ■ Mark Pullen

The various Defense IT trade journals are offering increasingly nuanced discussions of how open source software (OSS), service oriented architecture (SOA), Agile software development, and the "cloud" concept can and should be applied to streamline, accelerate, and improve the defense enterprise (DE) IT acquisition process. It is refreshing to see these subtly nuanced and pragmatic views in lieu of the "religious" black-and-white arguments that had here-to-fore been typical in the defense-related IT literature. However, generally absent are discussions of widespread success at these various modern IT paradigms within the DE. Why is that?

Our sense is that the DE has indeed little widespread success at deploying modern IT paradigms such as SOA, OSS, "cloud," or "Agile." In our view, the elephant in the room is that to leverage any of these at scale, the DE must be generally competent to field large IT systems. Clearly, that is not the case. If the myriad GAO and Defense Science Board (DSB) reports over the last decade were not sufficiently convincing, surely the 2010 National Defense Authorization Act (NDAA) Section 804 is.

Section 804 is a succinct mandate requiring OSD to explain to Congress how it aims to finally fix its IT acquisition process. In response to Section 804, OSD has submitted its November 2010 report (*A New Approach for Delivering IT Capability to the DoD*) and established an IT Acquisition Reform Task Force (IT-TF). The IT-TF reports to Deputy Secretary of Defense William Lynn and is led by Deputy Chief Management Officer Elizabeth McGrath.

We believe that Lynn's and McGrath's success at responding to the congressional mandate will depend on their ability to address Einstein's dilemma. Recall that Einstein thought trying to solve a problem with the same approach that created the problem was crazy. It seems to us that Defense leaders should take a cue from Einstein and ask themselves why the dozens of previous reports, roadmaps, and mandates aimed at fixing aspects of Defense IT acquisition have not led to the envisioned successes. Perhaps it is because the tacit assumption made by these reports is that the as-is/to-be gap can and will be bridged by the existing Pentagon processes. So far, that assumption has proven false. Einstein might have said that it is time for new assumptions.

One effective technique—arguably the most effective technique—for mitigating risk in any new initiative is to assign the best person to the project, free him or her from other responsibilities, allow him or her to pick an elite team, and empower the team with sufficient resources and top cover to succeed. This is the approach good leaders invariably apply when the stakes are high.

'Sgt. Rock! Pick your best five soldiers and TAKE THAT HILL! We'll cover you.'

The typical approach to executing a new initiative within the DE bureaucracy is to assign it as additional duty to an already overtasked senior executive. That senior executive inevitably establishes a working group(s). The working group is composed either of "stuckees" involuntarily assigned for various reasons (rarely associated with expertise), or volunteers who choose to join the project because they have a vested interest.

The working group meets on a regular schedule. It eventually delivers a report of some sort. Any subsequent success "on the ground" requires that someone actually read the report and do something about it. In our experience with this approach, success is rare.

Einstein might have suggested that OSD should try the former approach this time around—i.e., find the metaphorical Sgt. Rock, tell him/her to take the hill, and cover this person while she/he heroically does that.

Phenomena such as eBay, Amazon, Google, Travelocity, IRS eFile, Wikipedia, Facebook, the iPhone, Linux, and others have clearly influenced the thinking of Defense leadership. That is, Defense leaders have recognized how IT-related paradigms like SOA, Agile, cloud, and OSS have contributed to the massive success of these enterprises. Defense concepts like "net-centric operations/warfare" and, lately, "cyber operations/cyber warfare" aim to harvest similar success at scale through application of the same IT paradigms. Indeed, the Defense netcentric implementing policies and ensuing initiatives seem to be based on the notion that particular technologies can, in and of themselves, bring about desired outcomes. The hypothesis seems to be "If the DE provides generic technologically-

Gunderson *is a research associate professor of information science at the Naval Post Graduate School in Monterey, Calif. He retired from the Navy as a captain after 27 years of service, with various leadership roles in information system interoperability.* **Pullen** *is a professor of computer science and director of the Center of Excellence in Command, Control, Communications, Computing and Intelligence at George Mason University, Fairfax, Va. He previously was a program director at the Defense Advanced Research Projects Agency (DARPA).*

Defense leaders should take a cue from Einstein and ask themselves why the dozens of previous reports, roadmaps, and mandates aimed at fixing aspects of Defense IT acquisition have not led to the envisioned successes.

enabled network resources, then military programs will reap untold benefits."

However, in our research, we find very few people who argue that programs like Netcentric Enterprise Services (NCES), Defense Travel Service (DTS), Navy Marine Corps Intranet (NMCI), Defense Knowledge Online (DKO), the various "government open source" software repositories—not to mention the various C4ISR programs embracing SOA—have had the degree of success-at-scale of their commercial exemplars.

The various Defense netcentric policies and initiatives inevitably fail to recognize the fundamental fact that, in all the impressive exemplars, it is value proposition (VP) and the supporting business model that drives success at scale. In other words, technologies serve as catalysts *if and only if* they enhance the VP, business model, or both. For example, the travel business was flourishing long before Travelocity entered the picture. Travelocity decreased time and cost associated with existing lucrative transactions by applying web services and service architecture. Likewise, Amazon, eBay, and IRS eFile, within their chosen domains. Collaborative portals such as Java.net and SourceForge allow compelling OSS projects to scale globally. Non-compelling OSS projects wither and die on the same collaborative portals that support the massively successful projects, as do non-compelling Wiki sites.

In other words, technologists can fuel success when they follow the money. By carefully observing existing patterns of transactions, providing tools that reduce barriers to those transactions, and expanding the market space, IT practitioners can fan sparks into bonfires by providing "enterprise" capabilities. However, they need to start where the sparks already exist.

Therefore, Einstein might have suggested that the DE stop pushing particular technologies, and focus on "market forces." That is, for the DE to succeed with OSS, SOA, cloud, Agile, etc, the DE must seek out existing "commerce" among members of the defense community that might benefit from better IT tools. Studying the existing functional transaction space will enable discovery of VPs and enabling business models—that is, "acquisition strategies"—that resonate within a particular ecosystem of competent and empowered providers and consumers of the required IT capabilities.

Study of success cases reveals that an effective business model/acquisition strategy inevitably recognizes two basic truths: you get what you measure, and you get what you pay for. Measuring the right things and then contracting for the right things are both critical to success. Today the DE measures compliance with bureaucratic requirements and size of empire. DE executes its program and budget accordingly. DE programs outsource engineering of very large complex systems, via long serial processes. Hence, DE programs tend to deliver capability that is archaic, late, and over budget.

Needed Changes for Needed Outcomes

What fundamental changes to that "outsource-your-brains-and-measure-compliance" model will catalyze the desired fundamental changes in program output?

At least one DE community of practice is embracing this Einsteinian approach to IT Acquisition Reform. Members of the USN and USMC Intelligence Community, under the Aegis of the Section 804 mandate, are establishing what they call a Naval-Intelligence Capability Evolution (N-ICE) Pilot Portfolio. The HQ Marine Corps director of intelligence, and the USN Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I) Principal Deputy for Intelligence, are the leaders of this community. Their near-term objective is to deliver critical persistent intelligence, surveillance, and reconnaissance (PISR) to blue forces on the tactical edge in Afghanistan.

Generally, the N-ICE value proposition is better speed to better capability. The industrial jargon for this universally accepted approach is time to value. For a fixed IT budget, the objective is to optimize Value of Acquisition (VoA), where:

VoA = (value per capability) x (number of capabilities) ÷ (calendar time to develop/test/certify) ÷ (cost).

Value is the critical parameter. Given that for N-ICE, the application domain is intelligence, value is most likely to be associated with the quality of collection, processing, and delivery of information. Time and cost either enhance or detract from basic value. If either time or cost grows to the point where VoA drops below some threshold value, it is time to walk away from sunk costs, and/or de-scope the effort, in order to get something useful in the warfighters' hands in time to make a difference.

Generally the N-ICE business model is value-off-the-shelf (VOTS). Off-the-Shelf (OTS) means a capability is readily consumable—that it is pre-certified for DE use, is available via convenient procurement vehicle, works out of the box, and comes with life cycle support. The N-ICE approach is to: (1) buy down as much risk as possible with pure OTS capability and deploy that capability immediately; (2) identify specific gaps between existing OTS capability and the total requirement; (3) close the OTS gap by investing within the COTS ecosystem to develop new OTS capabilities.

In this model, it is critically important that the government retain full intellectual property rights to the IT the government pays to develop. One good way to do that is to require developers to use open source licenses for government-developed components. In any case, this approach requires an objectively specified "modular open systems approach" ("MOSA," which is un-defined jargon in many DE IT policy documents). The industrial best practice re MOSA is called "product line architecture" (PLA). PLA provides detailed technical specifications for persistent modular IT "platforms." The IT platform plug-and-play specifications, then, allows efficient re-use of components and enables lucrative time-to-value for multiple IT-enabled enterprises.

Apple iPhone, iPad, and iPod, and MacBooks all share the same PLA, for example. Google and Microsoft likewise specify their own versions of PLA. In industrial PLA "open" is obviously a relative term. Consider, for example, iPhone's proprietary development environment vs. Android's open source environment. Both are "open" to their own large diverse ecosystems of developers. However, in every case of effective PLA, "open" is described objectively and in great technical detail. That is not the case in most defense system architectures.

The VP of PLA for provider enterprises is that it can prevent internal verticals from competing with each other on the basis of basic infrastructure. Rather, enterprise PLA allows internal verticals to efficiently differentiate themselves at the application level. The VP of PLA for consuming enterprises is that it allows a single point of access to a multitude of capability providers—preventing lock-in to any particular provider. (Regardless of whether you like Mac or Window, iPhone or Android, you can have your choice of any number of competing application solution providers.) Significantly, in the traditional approach to defense acquisition, all the provider enterprise verticals—the individual programs—have no incentive or central governance structure to cause them to build on a common PLA. They do indeed compete with each other, in the Pentagon process, for the resources to build their own closed infrastructure. Members of the defense consumer enterprise are locked in, either by regulation or tradition, to particular providers. Again, Einstein might suggest that a fundamental change is in order.

The N-ICE business model recognizes the need to make this fundamental change. Further, the N-ICE community recognizes that information assurance (IA) and information interoperability (IoP), and the ironclad requirement to certify systems for both, are long poles for all defense acquisition activities. Any improvement to the current arcane, artisan, approach to IA and IoP certification would be universally considered a lucrative VP. Accordingly, the N-ICE approach applies emerging virtualization and semantic technology to build IA and IoP into its PLA. The N-ICE community of practice includes experts at the NSA and experts at the Joint Interoperability Test Command (JITC), who are vested in the success of this approach.

In our view, the elephant in the room is that to leverage any of these at scale, the DE must be generally competent to field large IT systems. Clearly, that is not the case.

The George Mason University Command, Control, Communications, Computers, and Intelligence (GMU C4I) Center is also a member of the N-ICE community of practice. On one hand, the GMU C4I Center has embraced the general PLA VP to address the issues of life cycle maintenance (LCM) for military MOSA. On the other hand, the center (and its partners) are applying OSS, Agile development, and Internet collaborative technologies according to their version of the VOTS business model. This approach considers LCM to be an end-to-end process that:

- Includes operational customers as partners in a continuous requirement capture → development/discovery of capability → T&E/V&V/certification → deployment feedback loop
- Recognizes that requirements for IA and Interoperability provide high barriers to entry for industry at large, add cost, and slow acquisition.
- Provides a virtual distributed, on line, low cost, non-proprietary Open Standard Test Framework (OSTF) that includes:
  - — Configurable instance(s) of military PLA
  - — Open source software development kits (SDKs) for IA and IoP components.
- Agile, OSS collaborative engineering environment allows/enforces continuously improving streamlined workflow across ecosystem of provider, consumers, and certifiers.

The N-ICE initiative, through the GMU C4I contribution described, aims to create an Einsteinian portal from the as-is, massive, serial, ponderous Defense IT acquisition process, to the to-be, lean, parallel, agile, process. In this case, "open" means open. Please join us.

The authors can be contacted at **cgunders@nps.edu** *and* **mpullen@c4i.gmu.edu.**